

AUG 21 2019

19-2603 BPG

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

BY

K.C.

DEPUTY

I, Special Agent Mathew L. Bryant, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—four electronic devices, further described in Attachment A—currently in law enforcement custody, and the extraction from that property of electronically stored information, further described in Attachment B.

2. The property to be searched is specifically identified as:

- a. A black Alcatel cell phone (**Device 1**) (**DEA Exhibit N-1**);
- b. A silver Samsung cell phone (**Device 2**) (**DEA Exhibit N-2**);
- c. A black Apple iPhone (**Device 3**) (**DEA Exhibit N-3**); and
- d. A black Samsung cell phone with International Mobile Equipment Identity (“IMEI”) #353302090798391 (**Device 4**) (**DEA Exhibit N-4**).

3. I am employed as a Special Agent with the United States Drug Enforcement Agency (“DEA”) and have been so employed since June 2017. I am currently assigned to the High Intensity Drug Trafficking Area (“HIDTA”) Group 51 of DEA’s Baltimore District Office. I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7)—that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. § 2516.

4. As part of my employment with DEA, I attended the Basic Agent Training Program, a 20-week resident program that included academic instruction in the basics of report writing, law, firearms, surveillance techniques, interview and interrogation techniques, automated information systems, drug identification, defensive tactics, and leadership and ethics. Prior to

JL

joining DEA, I was a police officer with the Metropolitan Police Department (in Washington, D.C.) for over 4 years, and a member of the Sixth District Crime Suppression Unit for more than 1 year. As a result of my law enforcement experience, I have had the opportunity to author search warrants and work with other experienced law enforcement officers.

5. I have a Master's Degree in criminal justice. As part of that degree program, I received a substantial amount of classroom training on constitutional rights. I also have a bachelor's degree in criminal justice. As part of that degree program, I studied and was instructed on U.S. law enforcement ethics.

6. Through my training, education, experience, and the experience of those with whom I work, I have become familiar with street sales of illicit drugs; the use of "stash" and "stash houses"; the prices, quantities, and packaging of illicit drugs; the use of couriers in the distribution of illicit drugs; drug traffickers' methods and modes of communication and the counter-surveillance techniques they employ; drug traffickers' language, terminology, traits, actions, and codes; the manufacturing and processing of controlled dangerous substances ("CDS"); and methods of asset concealment utilized by dealers of illicit drugs. Based on my training and experience, I know that narcotics dealers often use multiple cellular telephones for the purpose of communicating with sources of supply as well as communicating with customers.

7. I have participated in the execution of numerous search and seizure warrants yielding large amounts of CDS and leading to the arrests of numerous persons for violations of the CDS laws. In addition, through my investigative experience, I know that persons involved in the illegal distribution of CDS keep and maintain records of their various unlawful activities. My experience in similar cases has established that such records are regularly concealed in suspects' automobiles, residences, offices, and on their persons, or in warehouses and storage lockers. And

these records also take various forms—including both physical and electronic. Records commonly concealed by traffickers include, but are not limited to, notes in code, deposit slips, wired money transactions, savings pass books, hidden bank accounts, photographs of CDS and co-conspirators, various forms of commercial paper, personal address books, notebooks, receipts, ledgers, travel receipts (rental receipts, airline tickets, bus tickets, and/or train tickets) for both commercial and private travel, money orders and other papers relating to the ordering, transportation, sale, and distribution of CDS, and other documents that identify co-conspirators. The aforementioned records are usually kept in locations that are considered safe by drug traffickers—including in residences, vehicles, and on their persons—and where they have ready access to them.

8. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. Because I submit this affidavit for the limited purpose of obtaining the requested warrant, I have not included each and every fact known to me or my fellow investigators about the investigation. Instead, I have set forth only those facts that I believe are necessary to show there is probable cause for the requested warrant. I have not, however, excluded any information known to me that would defeat a finding of probable cause.

9. Based on the facts set forth in this affidavit, I submit there is probable cause to believe that the electronically stored information described in Attachment B is recorded on the electronic devices described in Attachment A. Specifically, I submit there is probable cause to believe that **Devices 1 through 4** have been used by Larry COATES in connection with a with a conspiracy to distribute and to possess with intent to distribute cocaine, in violation of 21 U.S.C. § 846; and furthermore, there is probable cause to believe that a search of **Devices 1 through 4**

will reveal evidence, fruits, and instrumentalities of the aforementioned crimes, and lead to the identification of individuals who are engaged in the commission of related offenses.

PROBABLE CAUSE

10. On September 26, 2018, U.S. Magistrate Judge Michael M. Anello, of the Southern District of California, authorized the Title III wiretap of, among other target telephones (“TT”), the phone assigned call number 424-200-3242 (TT-5), used by Sergio Antonio VILLASENOR. See Case No. 18-MC-0958 (sealed). Interception of TT-5 began the same day.

11. During the intercepts of VILLASENOR (TT-5), numerous calls were intercepted between VILLASENOR and COATES, who was utilizing two phone numbers: 410-980-4750 and 240-485-9500. Both phones are subscribed to COATES, at 144 Pinecove Ave, Odenton, MD. The intercepts between VILLASENOR and COATES began on September 27, 2018. Based on the intercepted calls, as well as multimedia messaging service (“MMS”) messages, investigators determined that VILLASENOR was shipping multi-pound quantities of cocaine from California to COATES in Maryland utilizing a shipping service. COATES was then utilizing the United States Postal Service (“USPS”), as well as United Parcel Service (“UPS”), to ship U.S. currency back to VILLASENOR in California.

12. For example, on November 9, 2018, VILLASENOR sent COATES a picture depicting what appeared to be 5 brick-shaped packages consistent in appearance with multiple kilograms of cocaine. COATES, in turn, sent VILLASENOR several pictures of shipment tracking information from USPS and UPS.

13. According to investigators who reviewed the communication between VILLASENOR and COATES, the following call took place on November 12, 2018, at

approximately 11:36 a.m.¹ VILLASENOR said he had been calling “the other one” but that COATES did not answer. COATES said he was at the gym working out. COATES said he put something in the [unintelligible (hereinafter, “U/I”)] UPS so he would send it once he was out of the gym. COATES asked if VILLASENOR heard him. VILLASENOR said no. COATES said he would send the confirmation when he got out of the gym. VILLASENOR asked how much COATES put “in there.” COATES said it was not that much since the banks were closed, so he could only do what he had. COATES said it was 18. VILLASENOR asked if COATES had not received any notes [U/I]. COATES said no. COATES said it had something to do with [U/I] send it back to him. COATES said it was not going to stop what he had going. COATES said the work came tomorrow. COATES said it would go towards the new [U/I]. VILLASENOR said okay. VILLASENOR said to give him a call when COATES was done. COATES said okay.

14. On November 12, 2018, COATES sent a picture of a UPS tracking label for a package weighing 3 lbs, 4.3 oz, with Tracking #1ZA9V9710112457164. Investigators obtained a manifest for the tracking number, which indicated the shipper was Staples Ship Center 01279, located at 7661 Arundel Mills Boulevard, Hanover, MD, and that the package would be shipped to Angel Picazo, 728 E. Florence Ave., Los Angeles, CA. The manifest also indicated the package was scanned into UPS’s possession on November 12, 2018, at 13:14 hours.

15. I later reviewed surveillance footage provided by the Staples store located at 7661 Arundel Mills Boulevard, in Hanover, MD. That footage shows an individual appearing to be COATES walking into the store on November 12, 2018, at approximately 1:13 pm. The individual was carrying a box in his right hand. At approximately 1:20 pm, the footage shows the same

¹ All times indicated are provided in Eastern Time, unless otherwise specified.

individual exiting the store and carrying a piece of paper in his right hand. The individual did not appear to be carrying a box out of the store.

16. Based upon the information obtained via wire intercepts, an investigator contacted a UPS employee assigned to its investigation division. Based on the tracking information, the employee advised that UPS had attempted to deliver the package to 728 E. Florence Ave., but there was no recipient present to sign for it, so UPS retained custody of the package at a shipping facility located at 1430 McKinley Ave., in Los Angeles, CA. On November 15, 2018, San Diego Superior Court Judge Jacqueline M. Stern authorized a warrant to search the package. Investigators executed it and seized \$18,000.00 in U.S. currency from inside the package.

17. According to investigators who reviewed communication between VILLASENOR and COATES, the following conversation took place between VILLASENOR and COATES on December 5, 2018. COATES stated that he (COATES) had just landed. VILLASENOR asked what all that noise was. COATES said he (COATES) was on the plane. VILLASENOR asked if COATES had that ticket with him; the ticket for the flight. COATES said yes, he (COATES) had his boarding pass. VILLASENOR asked for a picture. COATES said okay.

18. On December 10, 2018, U.S. Magistrate Judge Stephanie A. Gallagher issued a tracking warrant directing AT&T to provide prospective cell-site location information for the cellular telephone assigned the call number 410-980-4750 for a period of 45 days. See Case No. 18-3409-SAG (sealed). Using the data provided by AT&T pursuant to that warrant, along with other information, investigators located COATES in the Baltimore metropolitan area. Specifically, a social media search revealed multiple photographs of COATES and a female identified as Shawnte Miles, and a law enforcement database search indicated that Miles was

residing at 2614 Barred Owl Way, Odenton, MD. Location information from AT&T placed the 410-980-4750 device in the area surrounding 2614 Barred Owl Way.

19. On December 19, 2018, officers took up various positions in the 2600 block of Barred Owl Way in an attempt to conduct visual surveillance of COATES. At approximately 7 pm, they observed COATES exit 2614 Barred Owl Way, walk down the street, and enter the driver's door of his vehicle a Ford truck. Officers observed that no one else was present in the vehicle. They continued to surveil him and, at approximately 8:34 pm, officers observed COATES briefly park his vehicle in the Safeway parking lot located at 7643 Arundel Mills Boulevard, in Hanover, MD. Approximately two minutes later, officers observed a black BMW bearing Maryland temporary registration card T739526 park next to COATES's vehicle. Officers then observed that an unidentified male had approached COATES's vehicle. An officer then observed the unidentified male's hands near the driver's side window of COATES's vehicle. The officer then observed the unidentified male carrying a black bag approximately the size of a backpack. The unidentified male then placed the bag in the trunk of the BMW. Both vehicles left the parking lot immediately after the exchange.

20. I know from my training, experience, and working with other experienced investigators that individuals who engage in illegal CDS distribution will often meet for a brief period of time. During these brief meetings, individuals typically exchange CDS, U.S. currency, or both.

21. According to investigators who reviewed communication between VILLASENOR and COATES, the following conversation took place between VILLASENOR and COATES on December 24, 2018, at approximately 11:41 am. VILLASENOR stated he was expecting papers from other people but he (VILLASENOR) did not get anything so he (VILLASENOR) was

wondering if COATES could do him (VILLASENOR) a favor and send something to Walmart. COATES said that was fine. VILLASENOR said the most COATES could do on Walmart was 2500. COATES asked if that was it. VILLASENOR said yes, that was the most COATES could do so he (VILLASENOR) was wondering if COATES could do him this favor. COATES asked if banks were open today. VILLASENOR said he (VILLASENOR) did not know. COATES said it could be, stock market was open today so the banks must open.

22. I know from my training, experience, and from working with other experienced investigators that individuals engaged illegal CDS distribution will often refer to U.S. currency as "papers." Based on my training, experience, and from working with other experienced investigators, I believe that, during the above-described conversation, VILLASENOR asked COATES to send \$2,500.00 in U.S. currency via Walmart in connection with one or more CDS transactions. I know that Walmart allows individuals to transfer money to any location in the United States via Walmart2Walmart or MoneyGram. An individual can enter a Walmart store and conduct a money transfer in the customer service area. After conducting a money transfer, Walmart will provide the customer with a reference number and a receipt of purchase. On numerous occasions during this investigation, officers have observed COATES present in the customer service area of one or more Walmart stores.

23. According to investigators who reviewed communication between VILLASENOR and COATES, the following conversation took place between VILLASENOR and COATES on December 24, 2018, at approximately 12:57 pm. VILLASENOR asked if COATES talked to him. COATES said yes, he (COATES) just came out the bank. VILLASENOR asked whether COATES did it already. COATES said he (COATES) just did it so that was why he (COATES) could not answer the phone; he was at the teller. VILLASENOR said okay.

a. On December 24, 2018, at approximately 12:31 pm, officers observed COATES walk into the Bank of America located at 7045 Arundel Mills Boulevard, Hanover, MD.

b. I know that banks often will provide their customers with a receipt for any deposit transactions that are conducted. Based on my training, experience, knowledge of this investigation, and on working with other experienced investigators, I believe that VILLASENOR was asking COATES if he had been able to make a money deposit at a banking institution, and that COATES told him that he had. COATES also referred to a "teller," which is often used as shorthand for a bank teller.

24. U.S. Magistrate Judge J. Mark Coulson signed a warrant authorizing law enforcement to attach a GPS tracking device to COATES's Ford truck on December 21, 2018. See Case No. 18-3564-JMC (sealed). On December 26, 2018, investigators were able to safely attach the court-authorized GPS tracking device to the truck.

25. On January 15, 2019, officers were conducting surveillance of COATES with the assistance of the tracking device attached to COATES's vehicle. At approximately 7:20 pm, officers observed COATES enter his vehicle from the driveway of 7897 Bastille Place, Severn, MD. Officers then began mobile surveillance.

26. At approximately 7:30 pm, officers observed COATES park his vehicle in the 100 block of Pinecove Avenue, Odenton, MD. At some point shortly thereafter, officers observed that COATES had exited his vehicle. But at approximately 8:10 pm, officers observed COATES re-enter his vehicle and begin driving it from the 100 block of Pinecove Avenue. Officers could see that COATES was the only occupant of the vehicle. They then followed COATES until he parked the vehicle in the 2000 block of Westport Street, Baltimore, MD.

27. While COATES was parked in the 2000 block of Westport Street, an officer observed a female, later identified by Maryland driver's license as Ashley SNOWDEN, exiting the driver's door of a black Audi bearing Maryland license plate 3DF4369 (registered to SNOWDEN). SNOWDEN approached COATES's vehicle and opened the passenger door. The officer observed that SNOWDEN did not have any objects in her possession as she approached COATES's vehicle. The officer then observed SNOWDEN reach into COATES's vehicle and receive a black bag from COATES. With the black bag in her possession, SNOWDEN walked away from COATES's vehicle, entered the black Audi, and began driving away.

28. Investigators then began mobile surveillance of SNOWDEN until officers from the Baltimore County Police Department conducted a traffic stop in the 9400 block of Common Brook Road, Owings Mills, MD, on the basis of multiple traffic violations. During the traffic stop, an officer observed SNOWDEN reach into the center of the vehicle and then reach under the driver's seat. SNOWDEN told the officer that she had something in the car underneath the driver's seat. SNOWDEN then retrieved a black bag from underneath the driver's seat and handed it to the officer. The black bag was open and the officer immediately observed what he believed to be cocaine inside the bag. After SNOWDEN told the officer that he could have the bag, it was searched and found to contain approximately 384 grams of suspected cocaine. SNOWDEN was issued a traffic citation but not arrested or charged criminally.

29. According to investigators who reviewed the communication between VILLASENOR and COATES, the following conversation took place between VILLASENOR and COATES on January 29, 2019 at approximately 6:35 pm. VILLASENOR asked if he (COATES) had any tickets with him (COATES). COATES asked what he (VILLASENOR) meant by tickets. VILLASENOR said some papers. COATES said yes, he (COATES) had told him

(VILLASENOR) yesterday. VILLASENOR said he (VILLASENOR) had a little issue. VILLASENOR asked if he (COATES) could send him (VILLASENOR) 2,500 through Walmart. COATES said yes. VILLASENOR said he (VILLASENOR) would send him (COATES) the information right now. COATES said okay. VILLASENOR then sent the following SMS message to COATES: "Carlos Tomas Sandoval 4243666181."

30. On January 29, 2019, U.S. Magistrate Judge A. David Copperthite signed a warrant authorizing law enforcement to continue monitoring and maintaining the GPS tracking device that had been attached to COATES's vehicle. See Case No. 19-0354-ADC (sealed).

31. On January 31, 2019, investigators were conducting surveillance of COATES with the assistance of the tracking device attached to COATES's vehicle. At approximately 4:55 pm, investigators observed COATES's vehicle parked in the parking lot located at 10794 Green Mountain Circle, Colombia, MD. COATES's vehicle was parked behind a black Chevrolet Avalanche bearing Maryland license plate 3CT9968. The Chevrolet Avalanche is registered to an individual named Darius WATERS. Not only have the wire intercepts described above revealed that VILLASENOR and WATERS have been in communication with each other, COATES's banking records also indicate that COATES has made numerous deposits in an account that belongs to WATERS.

32. At approximately 5:03 pm, an investigator observed COATES exit from the front passenger seat of the Chevrolet Avalanche. COATES then entered the driver's seat of his vehicle. Officers then began surveillance of WATERS. At approximately 5:07 pm, an officer observed the Chevrolet Avalanche parking in a lot located at 5533 Harpers Farm Road, Colombia, MD. At approximately 7:52 pm, an officer observed WATERS enter the driver's seat of the Chevrolet Avalanche; officers continued their mobile surveillance of WATERS.

33. Because officers were able to keep WATERS under constant surveillance, he was not observed stopping or meeting with any other subjects of the investigation until approximately 8:25 pm, by which time WATERS had driven his vehicle to the 2000 block of Westport Street, Baltimore, MD. After officers observed WATERS drive his vehicle onto Westport Street, they briefly lost sight of him. But once officers entered the 2000 block of Westport Street, they observed an unidentified female who matched the physical description of SNOWDEN exit the front passenger seat of the Chevrolet Avalanche, carrying a white bag. The female then entered the driver's seat of a Honda passenger vehicle bearing Maryland license plate 7CX8719. Investigators then began mobile surveillance of the Honda.

34. The female driver made multiple turns and "U-turns" while officers were following her vehicle. Based on my training and experience, I believe that the female was driving the vehicle in a manner designed to avoid surveillance. Officers ultimately lost sight of the vehicle and were unable to continue mobile surveillance. Later, officers conducted a database search regarding Maryland registration 7CX8719 and determined that the Honda passenger vehicle was a rental vehicle owned by Avis. An officer contacted Avis rental and discovered the vehicle was rented by SNOWDEN during the time of the surveillance.

35. On February 28, 2019, officers were conducting surveillance of COATES, including by monitoring the court-ordered tracking device on COATES's vehicle. At approximately 3:10 pm, an officer observed COATES sitting in his vehicle as it was parked in the lot located at 10856 Green Mountain Circle, Colombia, MD. An officer then observed COATES exit his vehicle with a box in his right hand. COATES then entered the front passenger seat of a black Chevrolet Avalanche that was parked nearby. Officers could see that someone was sitting

in the driver's seat of the Avalanche. An officer observed COATES and the unidentified driver examining the aforementioned box that COATES had brought into the vehicle.

36. At approximately 4:35 pm, COATES exited the Chevrolet Avalanche, but was not carrying any visible objects in his hands. The driver of the Chevrolet Avalanche then drove the vehicle away from the parking lot, and officers began mobile surveillance of the vehicle. The Chevrolet Avalanche was then stopped for a broken front windshield by an officer from the Columbia Police Department in the 1000 block of Twins River Road, in Colombia, MD. The driver identified himself through his Maryland driver's license as Darius WATERS. Based on the observations described above, the officer requested a canine scan, and a canine certified to detect the odor of CDS arrived on the scene soon thereafter. While conducting the scan, the canine alerted to the odor of CDS within the Chevrolet Avalanche.

37. After the positive canine alert, officers conducted a brief search of the Chevrolet Avalanche, but failed to locate any CDS in the vehicle. But the officers were unable to conduct an organized and thorough search due to traffic in the area and the vehicle's location.

38. During the traffic stop, officers observed COATES operating his vehicle in the area. COATES parked his vehicle in a lot close to the stop, and was observed watching the officers conduct the stop. COATES then exited his vehicle and appeared to be concealing himself behind shrubbery as he continued to observe the stop. As COATES eventually walked back to his vehicle, he appeared to be looking into other parked cars in the area. Based on my knowledge, training, experience, I believe that COATES was looking into other vehicles to see if other members of law enforcement were sitting in parked cars in the area.

39. Later that evening, law enforcement sought and obtained a warrant to search the Chevrolet Avalanche from Howard County District Court Judge Mary Reese. After conducting

that search, officers were unable to locate CDS in the vehicle. Officers did, however, find two large voids in the vehicle, near where the canine had alerted. Based on my knowledge, training, and experience, I believe that these voids were intended for use as concealed storage areas for CDS or currency, or both.

40. On June 28, 2019, a federal grand jury in the Southern District of California indicted COATES on two counts of conspiring to distribute 5 kilograms or more of cocaine, in violation of 21 U.S.C. § 846, and conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956. See Indictment, United States v. Villasenor, Case No. 19 CR 2441 WQH (S.D. Cal. June 28, 2019) (sealed). The Southern District of California issued a warrant authorizing COATES's arrest the same day.

41. On July 30, 2019, U.S. Magistrate Judge Stephanie A. Gallagher issued a search and seizure warrant for the premises located at 7897 Bastille Place, Severn, MD, where investigators believed COATES was residing.

42. On July 31, 2019, law enforcement officers executed the search and seizure warrant at 7897 Bastille Place, Severn, MD, and observed COATES standing in the front bedroom of the residence. Upon entering into the residence, officers determined that COATES was the only individual inside the residence, and COATES stated that he lived alone. Officers then searched the front bedroom where COATES was located, and recovered **Devices 1 through 4** from inside that room. COATES was later taken into custody pursuant to the arrest warrant issued by the Southern District of California.

43. Law enforcement had previously conducted toll analysis on two phone numbers that investigators believed were associated with cell phones in COATES's possession. That analysis revealed that COATES was utilizing both phone numbers: 410-980-4750 and 240-485-

9500 to communicate with VILLASENOR. The analysis also revealed that COATES utilized 410-980-4750 to communicate with phone numbers associated with SNOWDEN and WATERS.

44. **Devices 1 through 4** are currently in the lawful possession of DEA, and came into DEA possession when they were seized during the execution of the above-mentioned search warrant. While DEA might already have all necessary authority to examine **Devices 1 through 4**, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

45. **Devices 1 through 4** are currently in storage at an evidence locker located in HIDTA Group 51's office located in the District of Maryland. In my training and experience, I know that **Devices 1 through 4** have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when they first came into the possession of DEA.

ELECTRONIC DEVICES AND EVIDENCE

46. As stated above, I submit there is probable cause to search Devices 1 through 4 for the electronic records described in Attachment B for the reasons stated below.

47. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

48. Based on my knowledge, training, and experience, I know that electronic evidence, including computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years. Even when files have been deleted, they can be recovered months or years later using forensic tools. When

a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

49. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures; and virtual memory “swap” or paging files.² Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs also store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash-storage devices or other external storage media, and the times at which the computer was in use. Computer file systems can also record information about the dates files were created and the sequence in which they were created.

² Although it is technically possible to delete or erase this evidence, computer users typically do not because special software is required for that task.

50. As further described in Attachment B, the requested warrant would authorize searching and seizing not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the devices were used, the purpose of that use, who used them, and when. Thus, law enforcement forensic analyst(s) will need access to and review all data stored on the device, including all assisting software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices, in order to locate the information called for in Attachment B.

51. Moreover, files related to the purchasing and selling of controlled substances, as well as the movement of currency, found on computers and other electronic devices are usually obtained from the internet or cellular data networks using application software that often leaves files, logs, or file remnants that tend to show the identity of the person engaging in the conduct, as well as the method of location or creation of the data, search terms used, and the exchange, transfer, distribution, possession, or origin of the files. Files that have been viewed on the internet are sometimes automatically downloaded into a temporary internet directory or "cache." The internet browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed internet pages or if a user takes steps to delete them. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

52. "User attribution" evidence also can be found on an electronic device and is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the device at a relevant time. I also know from training and experience, for example, that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of internet connection at the residence.

53. Searching electronic devices seized pursuant to the requested warrants for the evidence described in the Attachment B may require a range of data analysis techniques. For example, information regarding user attribution or internet use is located in various operating system log files that are not easily located or reviewed. In addition, a person engaged in criminal activity will attempt to conceal evidence of the activity by “hiding” files or giving them deceptive names. As explained above, because the warrant calls for records of how a device has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of an electronic device for the things described in this warrant will likely require a search among all the data stored in storage media. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or “slack” space. This, too, makes it exceedingly likely that it will be necessary here to use more thorough techniques.

54. And in searching for evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

55. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the computer and the application of knowledge about how the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

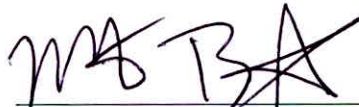
56. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

57. *Manner of execution.* Because the requested warrant would authorize officers to examine a device already in law enforcement's possession, execution of the warrant would not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time of the day or night.

19 - 2603 BPG

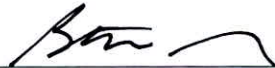
CONCLUSION

58. I respectfully submit this affidavit establishes probable cause to believe that the electronically stored information described in Attachment B is recorded on the devices described in Attachment A. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.



Special Agent Matthew Bryant
Drug Enforcement Administration

Sworn to and subscribed before me this 6TH day of August, 2019.



HONORABLE BETH P. GESNER
CHIEF UNITED STATES MAGISTRATE JUDGE

19 - 2603 BPG

ATTACHMENT A
Property to Be Searched

The property to be searched is specifically identified as:

- a. A black Alcatel cell phone (**Device 1**) (**DEA Exhibit N-1**);
 - b. A silver Samsung cell phone (**Device 2**) (**DEA Exhibit N-2**);
 - c. A black Apple iPhone (**Device 3**) (**DEA Exhibit N-3**); and
 - d. A black Samsung cell phone with International Mobile Equipment Identity (“IMEI”) #353302090798391 (**Device 4**) (**DEA Exhibit N-4**);
- located in HIDTA Group 51’s office in the District of Maryland.

ATTACHMENT B
Items to Be Seized

1. All records and information, in whatever form, including electronic, relating to violations of 21 U.S.C. § 846 involving Larry COATES since September 2018, including:

a. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

c. lists of and communication with customers and related identifying information;

d. any information relating to COATES's schedule or travel from September 1, 2018 to the present;

e. bank records, checks, credit card bills, account information, and other financial records.

2. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chats," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media; and

i. contextual information necessary to understand the evidence described in this attachment.

3. With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

a. surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

b. “opening” or cursorily reading the first few “pages” of such files in order to determine their precise contents;

c. “scanning” storage areas to discover and possibly recover recently deleted files;

d. “scanning” storage areas for deliberately hidden files; or

e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If, after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.